binarly

binarly.io

Mission Critical Protection: Binarly Enhances Security for Sonim Technologies Mobile Devices

Background

Sonim Technologies is a leading U.S. provider of ultra-rugged mobile devices designed for task workers operating in extreme, mission-critical environments. Trusted by police, first responders, and industrial teams, Sonim's devices deliver dependable communications when failure is not an option.

Committed to ethical supply chain practices and high integrity standards, Sonim ensures that every component in its rugged solutions meets strict cybersecurity requirements and assurances for telecom operators deploying devices into their networks.

The Challenge

Despite their physical durability, Sonim's devices are not immune to cybersecurity and software supply supply chain security risks. The company identified two key challenges:

I Hidden cyber threats

Traditional security tools failed to uncover deep-seated Android OS and firmware vulnerabilities. The threat of hidden backdoors and unverified components within the firmware posed significant risks to secure, dependable and always-available communications in environments where reliability is paramount.

II Compliance on a tight schedule

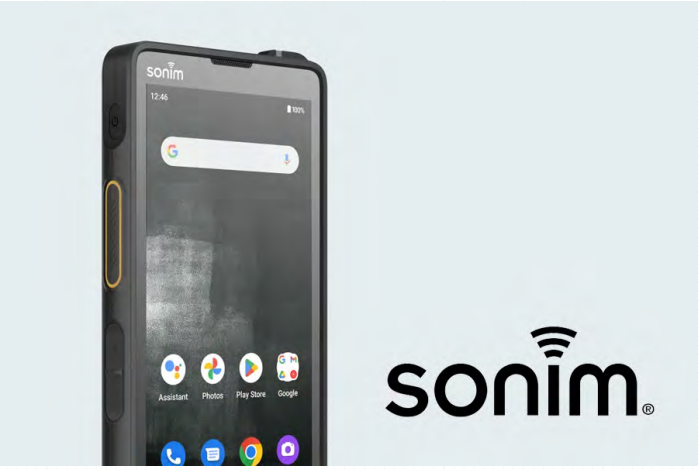
Increasing government and carrier security mandates required rapid generation of Software Bill of Materials (SBOMs) and comprehensive vulnerability reports. Manual processes were too slow, risking delays in obtaining essential certifications and carrier approvals.

The Partnership and Solution

To address these challenges, Sonim partnered with Binarly, a cybersecurity firm specializing in deep binary analysis, firmware integrity validation, and automated compliance reporting.

This collaboration provided Sonim with an integrated, automated solution to scan Android OS packages and firmware components to discover — and remediate — weak spots before they escalate into real-world exposure.

- **Automated Firmware Scanning**: Binarly conducts in-depth analysis of OS software and firmware to uncover both known vulnerabilities and hidden backdoors. This continuous scanning ensures that every piece of code is scrutinized, allowing Sonim to mitigate risks before mission-critical devices are shipped to customer segments.
- **Efficient SBOM Generation & Reporting**: Every firmware update now comes with an automatically generated, validated Software Bill of Material (SBOM). This transparency simplifies compliance verification for carriers and procurement teams, reducing manual effort and accelerating approval processes.
- **Seamless CI/CD Integration**: By integrating Binarly's API directly into Sonim's development pipeline, every firmware release is automatically scanned. This proactive approach means that security remains tight without hindering innovation or time-to-market.



The Binarly Transparency Platform provides the most comprehensive visibility into every layer of the software supply chain stack, including the Android OS. It includes patented technologies for the unique discovery of the cryptographic assets and generation of the most accurate CBOM to streamline PQC migration.

"Binarly's tools allow us to take a proactive approach to security," said **Harish Aithal, Senior Director Systems Architect at Sonim**. "By automating deep scans of our firmware and operating system, we can deliver devices that not only withstand physical extremes but also meet rigorous cybersecurity standards. This integration helps us protect our customers and streamline compliance processes."

The Wins

The Sonim–Binarly partnership has yielded tangible benefits:

- **Stronger security, faster compliance**: Android OS and firmware vulnerabilities are now identified and resolved early, while automated SBOMs and vulnerability reports cut down compliance time significantly. This streamlined process has led to faster carrier approvals and enhanced customer trust.
- **Operational reliability in critical scenarios**: Sonim's devices, now fortified with automated security measures, have proven their mettle in mission-critical operations. The enhanced security posture has ensured uninterrupted communication, even in the most challenging environments.
- **Proactive cybersecurity posture:** By automating deep Android OS and firmware analysis and integrating security checks into the development pipeline, Sonim has improved their cybersecurity posture — and that of their customers — by moving from reactively to proactively identifying software and firmware risks in their devices. This forward-thinking approach not only mitigates current risks but also sets the foundation for ongoing, robust security.

Conclusion

The partnership between Sonim Technologies and Binarly exemplifies how advanced cybersecurity can enhance rugged device innovation. For enterprises facing similar challenges in secure communications and compliance, the collaboration between Sonim and Binarly provides a proven model where software supply chain transparency can be achieved on hardware devices.

Sonim's commitment to proactive cybersecurity ensures that its devices remain a trusted lifeline for first responders and critical operations worldwide, demonstrating that even in the harshest environments, security and innovation can go hand in hand.

About Binarly

Binarly is a U.S.-based firmware and software supply chain security company founded in 2021. Our flagship Binarly Transparency Platform helps device manufacturers, OEMs, and enterprise product security teams detect vulnerabilities, misconfigurations, secrets, and malicious code in devices and software supply chains. Leveraging decades of research and program analysis expertise, we secure businesses, critical infrastructure, and consumers while assisting organizations in transitioning to a post-quantum cryptography (PQC) environment. For more information, visit **https://binarly.io**.